Alexicon
Evaluate – Innovate – Advocate

February 27, 2019

VIA ELECTRONIC COMMENT FILING SYSTEM (ECFS)

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, DC 20554

RE: EB Docket No. 06-36 - CPNI Certification Filing for
San Carlos Apache Telecommunications Utility, Inc.

Dear Ms. Dortch:

On behalf of San Carlos Apache Telecommunications Utility Inc. (499 Filer ID No. 815825), please find the attached annual CPNI certification and accompanying statement covering 2018 which is being filed pursuant to Commission Rule 64.2009(e).

Should you have any questions or need further assistance, please contact me at (918) 376-9901 or dion@alexicon.net .

Sincerely,

Dion Nero
Authorized Representative of
San Carlos Apache Telecommunications Utility, Inc.

DN/rs
Attachment

cc: Ms. Shirley Ortiz, San Carlos Apache Telecommunications Utility, Inc.

Annual 47 CFR § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 26, 2019

2. Name of company(s) covered by this certification: San Carlos Apache Telecommunications Utility, Inc.

3. Form 499 Filer ID: 815825

4. Name of signatory: Shirley Ortiz

5. Title of signatory: CEO/General Manager

6. Certification:

I, Shirley Ortiz, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company *has not* taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company *has not* received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures

ACCOMPANYING STATEMENT

This statement explains how San Carlos Apache Telecommunications Utility, Inc.'s ("the Company") procedures ensure compliance with the FCC rules on CPNI and FCC requirements for the safeguarding of such customer information.

The Company has chosen to prohibit the use or disclosure of CPNI for marketing purposes. If CPNI is to be used for its sales and marketing campaigns in the future, the required notice and opt-out approval process will be conducted as required, and safeguards will be implemented in accordance with 47 C.F.R. §64.2009.

The Company has a written CPNI Policy that explains, among other things, what CPNI is, when it may be used without customer approval, and when customer approval is required prior to CPNI being used, disclosed or accessed for marketing purposes.

The Company has assigned a Director for CPNI Compliance to serve as the central point of contact regarding the Company's CPNI responsibilities and questions related to CPNI Policy. The Director for CPNI Compliance has responsibilities including, but not limited to, supervising the training of all Company employees with access to CPNI, investigating complaints of unauthorized release of CPNI, and reporting any breaches to the appropriate law enforcement agencies. The Director for CPNI Compliance also has the responsibility to maintain CPNI records in accordance with FCC rules, including records of any discovered breaches, notifications of breaches to law enforcement, and law enforcements' responses to the notifications for a period of at least two years.

The Company has internal procedures in place to educate its employees about CPNI and the disclosure of CPNI. Employees with access to this information have been trained as to when they are and are not authorized to use CPNI. Any employee that uses, discloses, or permits access to CPNI in violation of Federal regulations is subject to disciplinary action, and possible termination, as described in the Company's CPNI Policy manual.

The Company requires express opt-in consent from a customer prior to the release of CPNI to a joint venture partner or independent contractor for marketing purposes. However, currently the Company does not disclose CPNI to any third party for marketing purposes.

Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F.R. §64.2010. Prior to the disclosure of CPNI, customers initiating calls to or visiting the Company's offices are properly authenticated. Passwords and password back-up authentication procedures for lost or forgotten

passwords have been implemented in accordance with §64.2010(e). For a new customer, the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical information or account information. Prior to establishing a password, the Company shall authenticate the customer by calling the customer back at their telephone number of record or reviewing a valid, photo ID that matches the name of the account if the customer is in the retail office.

Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, call detail information is only provided by sending it to the customer's address of record or by calling the customer at their telephone number of record. If the customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance, then the Company is permitted to discuss the call detail information provided by the customer to address the customer service issue. Prior to the Company disclosing CPNI to a customer visiting any of its retail offices in person, the customer must present a valid photo ID matching the customer's account information.

Currently customers do not have online access to their accounts. If that changes in the future, online access to CPNI will be provided to customers in compliance with §64.2010(d).

The Company has implemented procedures to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

In the event of a CPNI breach, the Company complies with the FCC's rules regarding notice to law enforcement (i.e., United States Secret Service and the Federal Bureau of Investigation) and customers. Records of any CPNI breach and notification to law enforcement, as well as law enforcement's responses, are maintained for a period of at least two years.